Properties of leader-laggard chaos synchronization in mutually coupled external-cavity semiconductor lasers

Ning Jiang,* Wei Pan, Bin Luo, Lianshan Yan, Shuiying Xiang, Lei Yang, Di Zheng, and Nianqiang Li
Center for Information Photonics and Communications, Southwest Jiaotong University, Cheng Du, Sichuan 610031, People's Republic of China

(Received 22 July 2009; revised manuscript received 12 April 2010; published 23 June 2010)

The properties of the leader-laggard chaos synchronization (LLCS) in two mutually coupled external-cavity semiconductor lasers are studied systematically. We theoretically analyze the general conditions for the LLCS based on the symmetric operation mechanism and numerically investigate the influences of operation parameters, the mismatch robustness, the chaos pass filtering effects, the communication performance, and the security of the system. It is demonstrated that stable LLCS, which allows simultaneous bidirectional message exchange in virtue of mutual chaos pass filtering effect, can be achieved in a wide operation region; moreover, high-quality LLCS and satisfactory communication performance can be maintained under a relatively large device parameter mismatch. Compared with the isochronal chaos synchronization in the same system, LLCS provides a wider operation region, a better mismatch robustness, and a stronger chaos pass filtering effect. In addition, the investigations on the security of private key message transmission under some potential attacks indicate that the security can be enhanced by increasing the bit rate moderately, exchanging messages with different bit rates, or monitoring the LLCS.

DOI: 10.1103/PhysRevE.81.066217 PACS number(s): 05.45.Pq, 42.55.Px, 42.60.Mi

I. INTRODUCTION

Chaos synchronization has attracted extensive attention since the end of the last century, for its potential applications in secure communications [1–6], neural networks [7], etc. In optical communication systems, external-cavity semiconductor laser (ECSL) [3–5] is a good candidate for the generation of broad-bandwidth chaotic carrier, which has been extensively investigated and used to realize the master-slave (unidirectional) optical chaotic communication systems [4,6]. In such systems, the message with small amplitude is encoded onto or into the chaotic carrier with appropriate encryption schemes (e.g., chaos masking [2], chaos shift keying [3,4], and chaos modulation [5–8]) at the transmitter end. At the receiver end, the message is extracted in virtue of the chaos pass filtering (CPF) effect [5,6,8,9]. The feasibility of this technique has been confirmed by the field experiment in Athens [9]. However, the prominent mismatch robustness of the injection-locking synchronization would degrade the security of the message transmission in the master-slave configuration. In Ref. [5], Li and co-workers demonstrated that the message transmitted in such a system can be decoded by a laser with 20% mismatch as long as the injection strength is sufficiently strong. Therefore, chaos communication systems with high transmission security are desired.

Mutually coupled semiconductor laser (MCSL) [10–12] system is an emerging topic in recent few years, which can improve the transmission security. Differing from the master-slave setup, the outputs of the MCSLs are synchronized under a unique mechanism, namely, the symmetric operation mechanism, which requires that the lasers as well as the external optical injections should be identical. Nevertheless, in the face-to-face MCSL configurations, the isochronal chaos synchronization (ICS) is unstable, and one laser has to be slightly detuned to obtain the well-defined leader-laggard synchronization [13]. Klein and co-workers demonstrated that stable ICS in MCSLs can be achieved by introducing self-feedback to each semiconductor laser (SL) [14], and they applied this concept into the public channel cryptography based on the mutual chaos pass filtering (MCPF) effect [15]. Recently, Vicente and colleagues provided a bidirectional information exchange scheme based on the leader-laggard chaos synchronization (LLCS) in two MCSLs [16], where a partially transparent mirror is positioned in between. Most of studies on the synchronization of MCSLs reported up to now mainly focused on the ICS [7,14,15], while a thorough investigation of the LLCS in mutually coupled ECSLs has not been performed. Several issues, such as synchronization conditions, synchronization characteristics, communication performance, and transmission security of the LLCS, motivate further investigation.

In this study, we concentrate on the properties of the LLCS in a system consisting of two mutually coupled ECSLs. The paper is organized as follows. Using the well-known Lang-Kobayashi equations, the conditions of the different types of synchronization will be first derived in Sec. II. In Sec. III, the operation ranges with stable synchronization as well as the system robustness against the parameter mismatches will be discussed in detail. CPF effects and the communication performance will be analyzed and evaluated in Sec. IV. Moreover, to clarify the difference between the LLCS and ICS which might occur in the same system, the synchronization and communication performances will be examined and compared. Section V will discuss the security of message transmission under some possible attacks, and some methods will be proposed to enhance the security. Finally, a conclusion of this study will be presented in Sec. VI.

*swjtu_nj@163.com

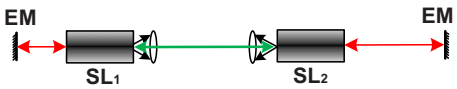

FIG. 1. (Color online) Schematic of two mutually coupled ECSLs. SL: semiconductor laser; EM: external mirror.

II. THEORY

The configuration of the mutually coupled ECSLs system is shown in Fig. 1. Two semiconductor lasers (SL1 and SL2) are mutually coupled via a public channel. Each of them simultaneously receives a delayed injection from the counterpart and a delayed self-feedback reflected from the external cavity. The chaotic carriers are generated by the joint contributions of the light feedback and injection. To mathematically describe the dynamic behaviors of the chaotic SLs, the Lang-Kobayashi equations [1–6,10–17] are modified by introducing corresponding terms representing the self-feedback and mutual coupling, respectively, which are written as

$$\dot{E}_j(t) = \frac{(1+i\alpha_j)}{2}\left(G_j - \frac{1}{\tau_{pj}}\right)E_j(t) + k_j E_j(t-\tau_j)\exp(i\omega_j\tau_j) + \sigma_j E_{3-j}(t-T)\exp(i\omega_{3-j}T)\exp(\mp i\Delta\omega t), \quad (1)$$

$$\dot{N}_j(t) = \frac{I}{q} - \frac{N_j(t)}{\tau_{ej}} - G_j|E_j(t)|^2, \quad (2)$$

where E is the slow varying complex electronic field, N is the carrier number, and the subscripts $j=1$ and 2 stand for SL1 and SL2, respectively. The other parameters are the optical gain G, the photon lifetime τ_p, the bias current I, the electric charge q, the carrier lifetime τ_e, and the linewidth enhancement factor α. The self-feedback and the mutual coupling are, respectively, modeled by the second term and the third term in the right-hand side of Eq. (1), wherein ω is the operating angular frequency, k is the feedback strength, σ is the mutual coupling strength, τ is the feedback delay, T is the injection flight time between SL1 and SL2, and $\Delta\omega = \omega_1 - \omega_2$ is the detuning frequency. Moreover, the signs – and + in the detuning term "$\mp\Delta\omega$" belong to SL1 and SL2, respectively. The optical gain G is defined as [6,16,17]

$$G_j = \frac{g_j[N(t) - N_{0j}]}{1 + s_j\|E_j(t)\|^2}, \quad (3)$$

where g is the differential gain, N_0 is the carrier number at transparency, and s is the gain suppression factor which characterizes the gain saturation effect.

According to the analysis method based on the symmetric operation mechanism [17,18], the relation between the synchronized SL1 and SL2 can be described as

$$E_1(t) = E_2(t+\Delta t), \quad (4)$$

$$N_1(t) = N_2(t+\Delta t). \quad (5)$$

Substituting Eqs. (4) and (5) into Eqs. (1) and (2), we obtain a general condition of synchronization between the MCSLs,

$$k_1E_1(t-\tau_1) + \sigma_1E_2(t-T) = k_2E_2(t+\Delta t-\tau_2) + \sigma_2E_1(t+\Delta t-T). \quad (6)$$

Here, Δt denotes the time lag between the outputs of SL1 and SL2. When $\Delta t>0$, SL1 synchronizes with SL2 but leads SL2 by Δt. When $\Delta t=0$, SL1 synchronizes with SL2 isochronally. Similarly, when $\Delta t<0$, SL1 and SL2 are synchronous but SL1 lags SL2 by Δt. The condition presented in Eq. (6) can be interpreted as the following two cases:

Case I:

$$k_1E_1(t-\tau_1) = k_2E_2(t+\Delta t-\tau_2),$$

$$\sigma_1E_2(t-T) = \sigma_2E_1(t+\Delta t-T). \quad (7)$$

Substituting Eq. (4) into Eq. (7),

$$k_1E_1(t-\tau_1) = k_2E_1(t-\tau_2),$$

$$\sigma_1E_2(t-T) = \sigma_2E_2(t+2\Delta t-T). \quad (8)$$

To satisfy this condition, the system parameters should meet,

$$k_1 = k_2,$$

$$\sigma_1 = \sigma_2,$$

$$\tau_1 = \tau_2. \quad (9)$$

Subsequently, the lag time between the MCSLs is

$$\Delta t = 0. \quad (10)$$

This is to say, the MCSLs synchronize isochronally. Moreover, when $\tau_1=\tau_2=T$, the synchronization conditions can be simplified to be $k_1+\sigma_1=k_2+\sigma_2$. This type of synchronization is the so-called ICS, as discussed in Refs [7,14,15,19,20].

Case II:

$$k_1E_1(t-\tau_1) = \sigma_2E_1(t+\Delta t-T),$$

$$\sigma_1E_2(t-T) = k_2E_2(t+\Delta t-\tau_2), \quad (11)$$

which can be realized if

$$k_1 = \sigma_2,$$

$$\sigma_1 = k_2,$$

$$\tau_1 + \tau_2 = 2T, \quad (12)$$

and the lag time between the MCSLs under this case is

$$\Delta t = T - \tau_1 = \tau_2 - T = \tfrac{1}{2}(\tau_2 - \tau_1). \quad (13)$$

Hence, the lag time is solely determined by the SLs' feedback delays in case II. We call this type of synchronization as LLCS. Equation (13) is a general formula for all mutual coupling systems that satisfy the conditions presented in Eq. (12). It is worth noting that the lag time of the LLCS is different from that of the generalized synchronization in master-slave systems, where the lag time equals the injection flight time [5].

To quantify the synchronization degree directly, we define the cross correlation function (CCF) $\rho(\tau)$ as Eq. (14), which

TABLE I. Values of parameters used in simulations [21,22].

Parameter	Symbol	Value
Operation wavelength	λ	1550 nm
Differential gain	g	1.5×10^{-8} ps^{-1}
Gain suppression factor	s	5×10^{-7}
Electron charge	q	1.602×10^{-19} C
Carrier lifetime in active region	τ_e	2 ns
Photon lifetime in active region	τ_p	2 ps
Transparency carrier density	N_0	1.5×10^8
Linewidth enhancement factor	α	5
Bias current	I	42 mA
Flight time between the SLs	T	5 ns
Feedback delay of SL1	τ_1	2 ns
Feedback delay of SL2	τ_2	8 ns

is obtained by calculating the correlation coefficient between the outputs of the SLs, as the output of SL1 is continuously shifted in time with respect to SL2 [4,14–17],

$$\rho(\tau)=\frac{\langle[P_1(t-\tau)-\langle P_1(t-\tau)\rangle][P_2(t)-\langle P_2(t)\rangle]\rangle}{\sqrt{\langle[P_1(t-\tau)-\langle P_1(t-\tau)\rangle]^2\rangle\langle[P_2(t)-\langle P_2(t)\rangle]^2\rangle}},\tag{14}$$

where $\langle\cdot\rangle$ denotes the time averaging, τ is the varying shift time, and $P=\|E\|^2$ is the photon number in the cavity. Theoretically, the maximum of CCF appears at $\tau=\Delta t$. On the other hand, we define the synchronization error as [5]

$$e=\frac{\langle\|P_1(t-\Delta t)-P_2(t)\|\rangle}{\langle P_1(t-\Delta t)\rangle}.\tag{15}$$

To handle this kind of differential equations in Eqs. (1) and (2), the general method is computer programming with Runge-Kutta algorithm. In this paper, a more direct method is adopted by establishing a visual simulation model with the object-oriented software package SIMULINK of MATLAB. In such a model, all functions are implemented conveniently by using the corresponding modules [4,5,11,17]. Unless otherwise stated, the values of the parameters used in our simulations are listed in Table I. Since the ICS has been extensively investigated, we mainly focus on the properties of LLCS in this study.

III. CHARACTERISTICS OF LEADER-LAGGARD CHAOS SYNCHRONIZATION

Figure 2 shows the temporal traces of the intensities of the MCSLs and the corresponding CCF. The chaotic output of SL1 leads that of SL2 by 3 ns [see Fig. 2(a)], which agrees with the result presented in Fig. 2(b), where the maximum peak occurs at 3 ns in the CCF diagram. These phenomena coincide with the theory formula (13) exactly. The diagram of the CCF is symmetric with respect to the lag time position because of the symmetric operation. The secondary peaks at ±5 ns are attributed to the injection-locking effect of mutual interaction, wherein the left secondary peak at -5 ns is

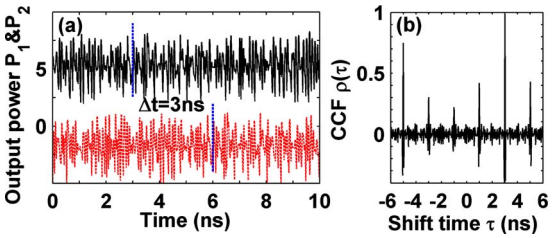

FIG. 2. (Color online) (a) Temporal traces of the optical power of SL1 (black solid curve) and SL2 (red dashed curve): here the trace of SL2 has been shifted vertically to distinguish from that of SL1, and the transient process has been compensated by shifting the traces horizontally; (b) the corresponding cross correlation function. Parameters: $k_1=\sigma_2=10$ ns^{-1} and $k_2=\sigma_1=15$ ns^{-1}.

higher than the right one at +5 ns. This is because that σ_1 (the strength of injection from SL2 to SL1) is larger than σ_2 (the strength of injection from SL1 to SL2), which results in the injection-locking effect of coupling from SL2 to SL1 is stronger than that of coupling from SL1 to SL2. Furthermore, there is no peak at the feedback delays in the CCF diagram, which means that the self-feedback does not affect the cross correlation directly. However, the contribution of the self-feedback is significant. If there is no self-feedback ($k_1=k_2=0$), the system is similar to the face-to-face configuration reported in Ref. [13], then each SL continues to receive a different signal $[\sigma_1E_2(t-T)\neq\sigma_2E_1(t-T)]$ from the counterpart SL. When the initial conditions are different, it is nearly impossible to keep the SLs' optical field and phase much close in (at least) a window of T; let synchronization along be maintained. Reversely, when each MCSL receives a self-feedback, the equation $dE_1(t)/dt=dE_2(t+\Delta t)/dt$ can be easily satisfied as long as the conditions in Eq. (12) are met [14]. Therefore, the necessary conditions for stable LLCS are $k_1>0$ and $k_2>0$.

To further explore the operation region for stable LLCS and the universality of the theoretical results, we investigate the dependence of the LLCS on the strengths of feedback and mutual coupling. As shown in Fig. 3(a), high-quality LLCS can be achieved over a wide range of the feedback and coupling strengths, as long as the conditions presented in Eq. (12) are met. The synchronization quality is degraded slightly as the mutual coupling strength and the self-feedback strength increase, because the increase in these strengths reinforces the difficulty to eliminate the effect of symmetry breaking induced by the initial condition differ-

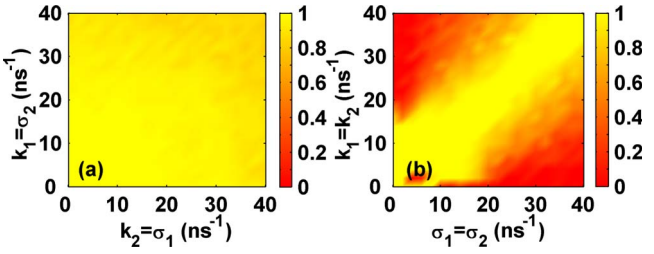

FIG. 3. (Color online) Maximum of the CCF as a function of the feedback strength and the mutual coupling strength: (a) result for the LLCS and (b) result for the ICS with $\tau_1=\tau_2=5$ ns.

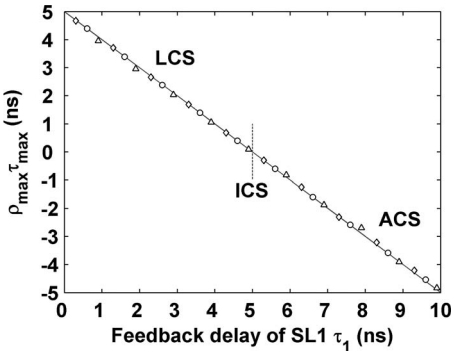

FIG. 4. Performance of the LLCS versus variation of the feedback delays for three different sets of coupling strength and feedback strength. LCS: lag chaos synchronization; ICS: isochronal chaos synchronization; ACS: anticipation chaos synchronization. The diamond, circle, and triangle dots stand for the cases of $k_1=\sigma_2=10$ ns^{-1} and $k_2=\sigma_1=15$ ns^{-1}, $k_1=k_2=\sigma_1=\sigma_2=10$ ns^{-1}, and $k_1=\sigma_2=10$ ns^{-1} and $k_2=\sigma_1=20$ ns^{-1}, respectively. The gray line denotes the theoretical result.

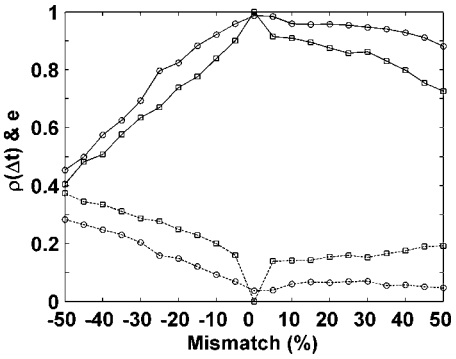

FIG. 5. The cross correlation $\rho(\Delta t)$ and the synchronization error e as functions of the parameter mismatch. The two circle curves, respectively, stand for the maximum of CCF (solid curve) and the synchronization error (dashed curve) for the LLCS with parameters identical to those of Fig. 2, while the two square curves denote those of the ICS with $k_1=k_2=\sigma_1=\sigma_2=15$ ns^{-1} and $\tau_1=\tau_2=T=5$ ns.

ence, namely, the "washout" of initial conditions as that in Ref. [23]. On the other hand, the result for the ICS in the same system is presented in Fig. 3(b). It is shown that stable ICS occurs when the feedback strengths are close to the mutual coupling strengths, which is in line with the results in Refs. [14,17]. The comparison between the results of the LLCS and those of the ICS indicates that the operation range of stable LLCS is much wider than that of ICS. Moreover, we have repeated the simulations for different feedback delays, and similar results are obtained.

Next we investigate the influences of the feedback delays on the performance of LLCS. Figure 4 depicts the synchronization performance of the LLCS for different feedback delays. Here, we introduce a parameter $\rho_{max}\tau_{max}$, which is defined as the product of the maximum of CCF and its corresponding position in the CCF diagram to indicate the performance of the LLCS quantitatively. Three different sets of feedback and mutual coupling strengths are considered. It is obvious that the simulation results well agree with the theoretical result with $\rho_{max}=1$ and $\tau_{max}=\Delta t=-\tau_1+5$ (gray line). Analyzing any point in the graph, we find that the shift time at which the maximum of CCF appears exactly agrees with Eq. (13). The fluctuation in the simulation results is due to the washout of initial conditions [23] and the finite simulation time (here, our simulation time is 400 ns). These results are in line with the experiment results in Ref. [24], where the mutual coupling system is composed of two SLs subject to optoelectronic feedback. Moreover, it is indicated that the feedback delays determine the leader and laggard roles. Specifically, the SL with short (long) external cavity serves as the leader (laggard). That is, when $\tau_1<\tau_2$, SL1 leads SL2 by Δt, and lag synchronization is achieved. Contrarily, when $\tau_1>\tau_2$, SL2 leads SL1, then anticipation synchronization takes place; when $\tau_1=\tau_2$, the LLCS turns to be ICS.

The physical mechanism of the LLCS and the ICS, namely, the symmetric operation, requires that SL1 is identical to SL2, which is similar to that of the complete synchronization in the master-slave systems. However, the complete synchronization is very sensitive to the parameter mismatch, which restricts the feasibility of its practical application [25]. For this reason, it is necessary to investigate the mismatch robustness of the LLCS to investigate the practical implement feasibility of the present scheme. Here, the mismatch is induced by increasing the N_0, s, and τ_e parameters and decreasing the g, τ_p, and α parameters of the SL2 by the same amount, as that in Ref. [26], which is mathematically described as $\alpha_2=(1-\mu)\alpha_1$, $g_2=(1-\mu)g_1$, $\tau_{p2}=(1-\mu)\tau_{p1}$, $N_{02}=(1+\mu)N_{01}$, $s_2=(1+\mu)s_1$, and $\tau_{e2}=(1+\mu)\tau_{e1}$, wherein μ stands for the mismatch ratio. Figure 5 shows the cross-correlation coefficient $\rho(\Delta t)$ (solid curve) and the corresponding synchronization error e (dashed curve) as functions of the mismatch ratio. The variation range of the mismatch ratio is from −50% to 50%. Apparently, high-quality LLCS with a correlation coefficient larger than 0.9 can be maintained as the mismatch ranges from −10% to 40%, even though the quality of the LLCS (circle) is degraded gradually with the increase in mismatch and the synchronization error increases correspondingly. For the sake of comparison, the mismatch robustness of the ICS in the same system (square) is also presented in Fig. 5. It is apparent that the ICS is more sensitive to the mismatch with respect to the LLCS. The ICS can just be maintained under some small mismatch (about −5% to 5%), and the synchronization quality is obviously worse than that of the LLCS. Therefore, the LLCS shows better mismatch robustness than the ICS.

IV. CHAOS PASS FILTERING AND MESSAGE TRANSMISSION

So far, we have observed high-quality synchronization, but it is not sufficient for the chaos-based communication. The message transmission needs another essential condition: the receiver is insensitive to the small perturbation added in (or on) the chaotic carrier transmitted from the transmitter. This phenomenon is the so-called CPF effect [5,6,8,9,27]. The stronger is the CPF effect, the easier is the recovery of message. For the message transmission in the present sys-

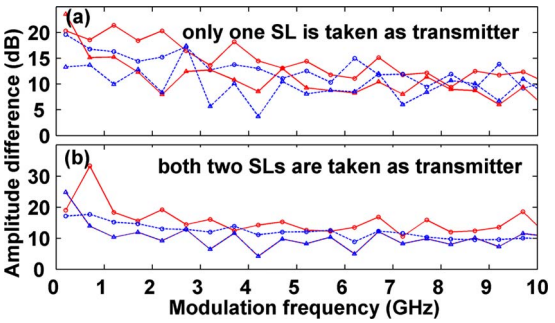

FIG. 6. (Color online) CPF effects of the MCSLs; (a) CPF effects of the two single-transmitter cases, wherein the two circle curves, respectively, stand for the CPF effects of case 1 (red solid curve) and case 2 (blue dashed curve) for the LLCS, while the two triangle curves denote those for the ICS in the same system. (b) MCPF effects of case 3, wherein the two circle curves, respectively, stand for the CPF effects of SL1 (blue dashed curve) and SL2 (red solid curve) for the LLCS, while the two triangle curves denote those for the ICS. The mutual coupling and feedback parameters are identical to those of Fig. 5.

tem, there are three cases: (1) only SL1 serves as the transmitter, (2) only SL2 serves as the transmitter, and (3) both lasers serve as the transmitters and receivers simultaneously. The CPF effects of the two single-transmitter cases (cases 1 and 2) allow for unidirectional message transmission, while that of case 3 is called MCPF in Refs. [15,17], which affords simultaneous bidirectional message exchange between the MCSLs [17].

Figure 6 shows the evaluations of the CPF effects of the three cases. Here, the transmitter is modulated by a small amplitude sinusoidal signal through external modulation [6]. Under such a scheme, the output of the transmitter multiples a term $1+0.07\sin(2\pi ft)$ before being injected to the receiver, wherein 0.07 is the modulation index and f is the modulation frequency. The degree of CPF effect is defined as the amplitude difference between the message component in the power spectrum of the modulated carrier (with message) of the transmitter, and that in the power spectrum of the receiver. Figure 6(a) presents the CPF effects of the two single-transmitter cases as a function of the message frequency f. Figure 6(b) shows the investigations of the MCPF effects, wherein the MCPF curves of the ICS (solid triangle and dashed triangle) are superposed for the symmetric configuration and identical dynamics. For all of the three transmission cases, each MCSL shows strong CPF effect. The CPF effects are weakened as the message frequency increases because of the reduction in the amplitude of the corresponding frequency component in the carrier. However, the CPF is still relatively strong when the message frequency is larger than the relaxation oscillation frequency at 3.43 GHz, which is different from that of the internal modulation case in Ref. [28], where the CPF is restricted by the relaxation oscillation frequency. This is because, under the external modulation, the amplitudes of the message components in the modulated carriers are not directly affected by the relaxation oscillation frequency, but related to the chaotic carriers' bandwidths that have been enhanced greatly by the self-feedback and the optical injection from the counterpart laser

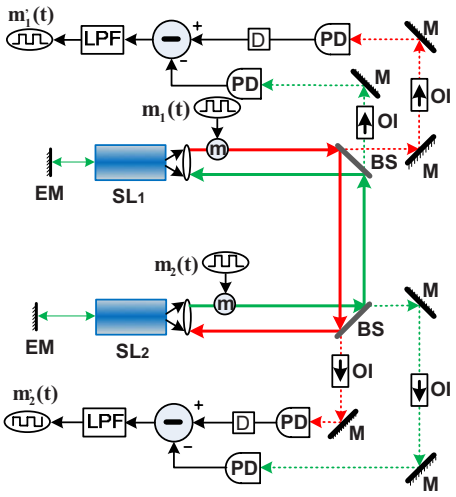

FIG. 7. (Color online) Schematic of chaos-based communication between two mutually coupled ECSLs. EM: external mirror; BS: beam splitter; M: mirror; m(t): original message; OI: optical isolator; PD: photodiode; D: time delay; LPF: low-passing filter; $m_1'(t)$ and $m_2'(t)$ stand for the recovered messages of SL1 and SL2, respectively.

as proved in Ref. [29]. Furthermore, the CPF effect of the laggard laser (SL2) is a little stronger than that of the leader one (SL1), because SL2 does not simultaneously reproduce the message transmitted from SL1. In addition, comparison between the results of the LLCS and those of the ICS (triangle curves) demonstrates that the LLCS provides a stronger CPF effect than the ICS. This is because that the symmetry requirement of the ICS is stricter than that of the LLCS. Therefore, it can be expected that the communication performance of the LLCS would be better than that of the ICS.

With the MCPF effects, we propose a scheme which allows the MCSLs to exchange message bidirectionally via a public channel, as shown in Fig. 7. This is a private key message encryption scheme, and the secret key consists of the system parameters as that in master-slave systems [2,5,9]. SL1 and SL2 stand for the communicating pair. At the transmitter end, the message is added into the chaotic carrier through chaos modulation, which is mathematically described as $P_{1m,2m}(t)=P_{1,2}(t)[1+Mm_{1,2}(t)]$ [5,6,21], where $P_m(t)$ is the modulated carrier transmitted on the public channel, $m(t)$ is the original message, and M is the modulation index which determines the message amplitude. At the receiver laser end, the message recovery is performed by subtracting the local chaotic carrier generated by receiver from the modulated carrier transmitted from the transmitter [5,6].

Figure 8 demonstrates the simultaneous bidirectional message transmission process in the proposed scheme. Here, the original messages (dashed curves) encrypted by SL1 and SL2 are two independent pseudorandom binary sequences (PRBS) with bit rate $B=1$ Gbit/s. The modulation index is set to 0.07 which is small enough to guarantee that the messages are well hidden in the chaotic carriers and the synchronization quality is not degraded apparently [$\rho(\Delta t)=0.96$]. In Fig. 8(a), we present the decryption process at the SL1 end, wherein the dashed curve stands for the original message

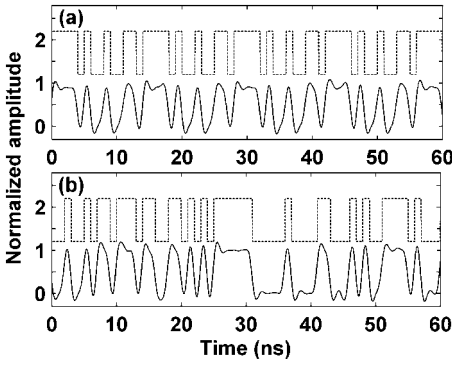

FIG. 8. Illustration of the message exchange process of LLCS. (a) The decryption at the SL1 end, wherein the dashed curve denotes the original message coded by SL2, and the solid curve represents the message recovered by SL1. (b) The decryption at the SL2 end, wherein the dashed curve denotes the original message coded by SL1, and the solid curve represents the message recovered by SL2. The mutual coupling and feedback parameters are identical to those of Fig. 2.

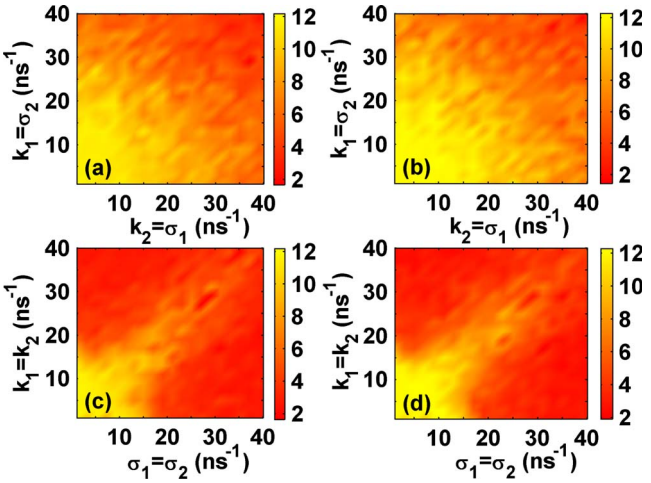

FIG. 9. (Color online) Communication performance (Q factor) as a function of the feedback strength and the mutual coupling strength for [(a) and (b)] the LLCS and [(c) and (d)] the ICS, wherein (a) and (c) show the Q factor of the message recovered by SL1, while (b) and (d) represent that of SL2.

encrypted by SL2, and the solid one denotes the recovered message of SL1. In the decryption process, the recovered message is filtered by a low-pass five-order Butterworth filter with a cutoff frequency of 0.6 GHz. Similarly, Fig. 8(b) shows the decryption process at the SL2 end. Apparently, the message encrypted by each MCSL can be successfully recovered by its counterpart laser. Moreover, repeating simulations with different feedback delays has indicated that the message exchange is not affected by the feedback delays.

In the following we investigate the communication performance of the proposed system. The general way used to evaluate the performance of a communication system is the bit error rate (BER) measurement. However, in simulations of the high-bit-rate systems such as the present system, the amount of calculation is very huge, such that it is difficult to calculate the BER with present common computers as explained in Ref. [30]. For an instance, more than 10^7 bits have to be considered for the BER estimation of a digital communication system with BER requirement of 10^{-6} and, moreover, the algorithm in the SIMULINK (Runge-Kutta algorithm) requires additional large amount of calculation. For these reasons, we adopt the calculation of Q factor to replace the BER characteristic. The Q-factor calculation is one of the most effective methods that can directly indicate the BER. A Q-factor value greater than 6 corresponds to satisfactory BER [30]. The Q-factor calculation is defined as

$$Q = \frac{\langle M_1 \rangle - \langle M_0 \rangle}{\varepsilon_1 - \varepsilon_0}, \tag{16}$$

where $\langle M_1 \rangle$ and $\langle M_0 \rangle$ stand for the average power of bits "1" bit and "0," respectively; ε_1 and ε_0 are the corresponding standard deviations.

Figure 9 presents the communication performance in the feedback strength and mutual coupling strength space. The original messages are identical to those of Fig. 8. For the LLCS case, satisfactory communication performance with a Q-factor value greater than 6 can be maintained over a wide range of the mutual coupling strengths and the feedback strengths as shown in Figs. 9(a) and 9(b), which coincides with the variation of the synchronization quality presented in Fig. 3(a). However, for the ICS case [Figs. 9(c) and 9(d)], when the feedback and the mutual coupling are strong, even though the synchronization quality is much high as shown in Fig. 3(b), the Q-factor values are degraded obviously. We attribute this phenomenon to the system symmetry degradation induced by the two independent PRBSs. When the mutual coupling is strong, the difference between the total external injections of the MCSLs, which is mainly determined by $M[\sigma_2 m_1(t) - \sigma_1 m_2(t)]$, is reinforced. Subsequently, the symmetry of the system is degraded, the synchronization quality of the chaotic carriers is deteriorated, and then the communication performance is degraded. This phenomenon does not happen under the LLCS scenario for the relatively relaxed symmetry requirement and stronger CPF effect (Fig. 6). Therefore, the operation region of message transmission based on the LLCS scheme is wider than that of the ICS.

Next, we investigate the influences of the amplitude and bit rate of message on the communication performance. The modulation index M determines the amplitude of message, and the bit rate B determines the base bandwidth of the message (the width of a single message bit). As shown in Fig. 10, there is a large region where the Q-factor values are greater than 6 for both cases of the LLCS and the ICS. When the modulation index is fixed, the Q factor is degraded gradually as the bit rate increases. For a fixed bit rate, a larger modulation index leads to a greater Q factor. For the LLCS case, the Q factor of message decrypted by SL2 [Fig. 10(b)] is a little better than that of SL1 [Fig. 10(a)] because of the stronger CPF as shown in Fig. 6. For the ICS case [Figs. 10(c) and 10(d)], the results are similar to those of the LLCS, while the Q factor is a little less than that of the LLCS for the weaker CPF. Analyzing several points in the high-bit-rate region, we find that part of the message bits can also be reproduced, but the BER increases apparently. In fact, the

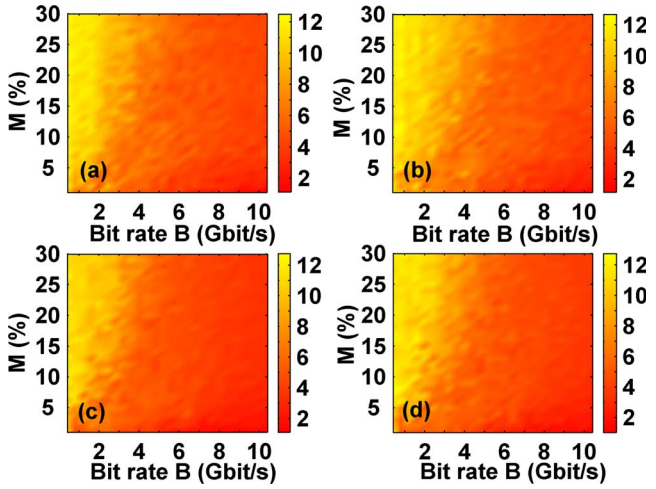

FIG. 10. (Color online) Communication performance (Q factor) as a function of the modulation index and the message bit rate. The top and bottom rows, respectively, denote the results of the LLCS and the ICS; (a) and (c) stand for the Q factor of the message recovered by SL1, while (b) and (d) stand for that of SL2. The mutual coupling and feedback parameters are identical to those of Fig. 5. The ranges of modulation index and bit rate are set to $M \in [1\%, 30\%]$ and $B \in [0.4, 10.4]$ (Gbits/s), respectively.

modulation index cannot be too large in practical applications, although a larger modulation index may provide a better message recovery. If the modulation index is larger than a certain limit, the synchronization between the SLs would be apparently degraded due to the affection of the messages, and the message may be extracted by a linear filtering with a cutoff frequency on the order of the bit rate.

Figure 11 shows the communication performance in the parameter space of the bit rate and the mismatch ratio. For the LLCS case [Figs. 11(a) and 11(b)], under some (even

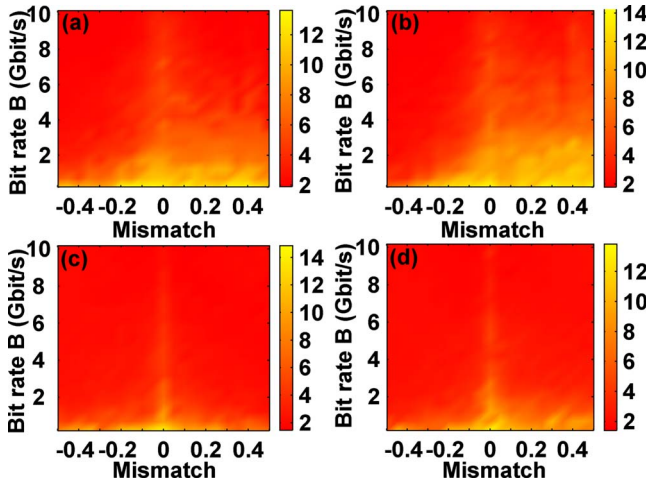

FIG. 11. (Color online) Communication performance as a function of bit rate and mismatch for the [(a) and (b)] LLCS and [(c) and (d)] ICS, wherein (a) and (c) show the Q factor of the recovery message of SL1, while (b) and (d) represent that of SL2. The mutual coupling and feedback parameters are identical to those of Fig. 5, and the modulation index is set to $M=7\%$. The range of bit rate is set to $B \in [0.2, 10.2]$ (Gbit/s).

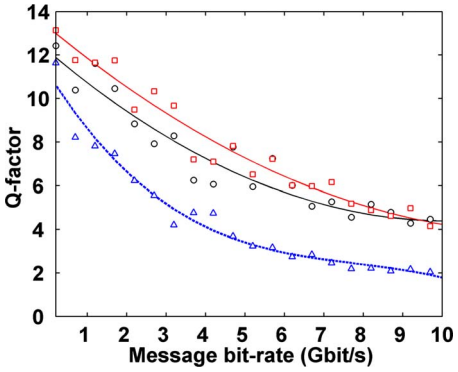

FIG. 12. (Color online) Communication performance of the legitimate communication SLs and the attacker; the circle, square, and triangle dots stand for the Q factor of the messages decrypted by SL1, SL2, and the attacker (SL3), respectively. The curves are the results of a polynomial fitting. The coupling and feedback parameters are identical to those of Fig. 2.

relatively large) mismatches the acceptable communication performance can be maintained when the bit rate is low. As the bit rate increases, the mismatch robustness region becomes narrower and narrower because of the weakened CPF effect (Fig. 6). The corresponding results for the ICS case [Figs. 11(c) and 11(d)] are similar, but the robustness region is much narrower and the Q-factor values are smaller with respect to those of the LLCS. These phenomena qualitatively verify the results in Fig. 5.

V. DISCUSSION OF THE SECURITY

Higher security is one of the main advantages of mutual coupling systems with respect to master-slave systems. Nevertheless, since the outputs of the MCSLs are accessible from the public channel (a simple beam splitter can easily separate the signals coming from SL1 and SL2), the system may suffer potential attacks such as using the amplified signals accessed from the public channel to lock a similar SL, listening in the public channel in both directions, using an ensemble of attackers, etc. In the following section, we discuss the security of the private key message encryption under some potential attacks scenarios and explore the corresponding solutions.

We first consider the scenario that the attacker locks to the amplified carriers $[P_{1m,2m}(t)]$ accessed from the public channel through injection locking. A semiconductor laser (SL3) having identical parameters as those of the legitimate lasers (SL1 and SL2) is taken as the hypothetical attacker who listens in the public channel from SL1 to SL2. The attacker SL3 is locked to the amplified modulation carrier $P_{1m}(t)$ through injection locking, which enables it to regenerate a chaotic carrier $P_3(t)$ and to extract the message in the manner of $P_{1m}(t)-P_3(t)$. Figure 12 shows the Q factor of the messages decrypted by the legitimate SLs and the attacker as a function of the message bit rate. It is apparent that the decryption performance of the attacker (triangle dots) is obviously worse than that of the legitimate communication SLs (square and circle dots). That is, the BER of the attacker is

higher than that of the legitimate SLs as that of Ref. [15], where the signal to noise ratios of the communicating parties and the attacker were compared. Moreover, when the bit rate is higher than 4 Gbits/s, the eavesdropped message is difficult to distinguish (when the Q factor is smaller than 4, the BER is much high). Therefore, the security can be further enhanced by increasing the bit rate moderately. The result is similar when the attacker listens in the transmission from SL2 to SL1.

Next we consider the scenario that the attacker listens in both directions of the public channel. In such a case, the attacker may intercept a message difference from the difference $P_{1m}(t-\Delta T)-P_{2m}(t)$, where ΔT is the difference between the delays from SL1 to the attacker and that from SL2 to the attacker, which is determined by the position at which the attacker breaks in the public channel. For this reason, the unidirectional message transmission between the MCSLs (cases 1 and 2 in the above section) is not secure, because the attacker can intercept the message directly. However, for the bidirectional message transmission (case 3), the attacker can only judge what message is transmitted when the message difference is 1 or -1 as proven in Refs. [6,16]. When the message difference is zero, the attacker has no idea of the message being transmitted. In this way, the legitimate communication SLs can negotiate a key through the public channel [16]. The probability that the attacker can correctly recover all message bits is $1/2^n$, where n is the number of the same bits coded by both SLs. That is, the more same bits are coded by both lasers (the greater the n), the higher is the security. From this point of view, the proposed system is also suitable for the enciphered data transmission, where several mistakes would corrupt the entire message. Furthermore, the message difference is a three-level sequence, and its base bandwidth is determined by

$$B_{\Delta m} = \mathrm{LCM}(B_1, B_2), \tag{17}$$

where LCM means computing the lowest common multiple. If the bit rate of message coded by SL1 is different from that of message coded by SL2 ($B_1 \neq B_2$), the message difference would not reveal the base bandwidths of the messages, such that it is difficult for the attacker to judge the bit widths of the messages. Under this scenario, even though the attacker knows what message is transmitted in the time slots of a duration $1/B_{\Delta m}$, this message is just a part of a bit, not a whole bit transmitted by the legitimate SLs. This way degrades the risk that the information in a whole bit duration is intercepted, such that the security is further improved. Moreover, if the messages are represented with return-to-zero code or polar codes (e.g., MANCHESTER code), the security can also be enhanced greatly.

Furthermore, since the lag time Δt is determined by the feedback delays, thus, it is necessary to investigate the security of the feedback delays. The privacy of the feedback delay has been a well-noted topic recently; several methods have been provided to enhance the privacy of the feedback delays, such as decreasing the feedback strength moderately, selecting proper injection current, and employing several external cavities [31–33]. In our simulations, we find that the feedback delays are secure for weak feedback with a feedback strength smaller than 7 ns^{-1}. On the other hand, it is worth mentioning that the attacker can estimate the precise lag time by calculating the cross correlation of the transmitted signals if and only if he accesses the transmitted signals at the center point of the public channel, because the lag time between $P_1(t-\Delta T)$ and $P_2(t)$ is $\Delta t+\Delta T$.

In addition, as proved in Sec. III, the maximum of CCF only occurs at the lag time Δt, such that the attack breakings occurring on the public channel will change the quality of the LLCS or change the position of Δt [6,17]. Based on this, we can easily detect whether the public channel is attacked by monitoring the quality and the lag time of the LLCS. If the quality of LLCS is degraded or the lag time is changed, the communicating SLs can maintain the security by interrupting the communication or switching channels.

Summarily, it is not easy to jeopardize the security of the private key message encryption in the present system. The mismatch robustness and high security of the LLCS reinforce the practical implement feasibility of secure optical communication in the proposed system.

VI. CONCLUSION

The chaos synchronization and communication in two mutually coupled semiconductor lasers subject to individual self-feedback have been investigated systematically. By analyzing the mutual coupling system with the symmetric operation mechanism, we have derived the general conditions for the existence of LLCS solution and found that the lag time is solely determined by the difference of feedback delays. The investigations on the CPF effects indicate that both MCSLs show strong CPF, while the CPF of the laggard SL is stronger than that of the leader one. On the other hand, the practical feasibility of the system is explored by considering the parameter mismatch in the investigations of synchronization performance and the message exchange processes, which demonstrates that high-quality LLCS and satisfactory communication performance can be maintained under some relatively large mismatches (of a few tens of percent). Comparing the properties of the LLCS with those of the ICS in the same system, we found that the LLCS shows a wider operation region, a better mismatch robustness, and a stronger CPF effect. Moreover, the security of the private key message transmission based on the LLCS is discussed, which shows that under some possible attack scenarios the security can be enhanced by several ways, such as increasing the bit rate moderately, transmitting messages with different bit rates on the public channel, or monitoring the LLCS.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No. 60976039), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20070613058), and the Doctoral Innovation Talent Foundation of Southwest Jiaotong University (2009). The authors acknowledge Dr. Weili Zhang, Dr. Xihua Zou, Dr. Xiaofeng Li, and the reviewers for their helpful guidance and suggestions.

[1] C. Juang, T. M. Hwang, J. Juang, and W. W. Lin, IEEE J. Quantum Electron. **36**, 300 (2000).
[2] G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998).
[3] C. R. Mirasso, J. Mulet, and C. Masoller, IEEE Photonics Technol. Lett. **14**, 456 (2002).
[4] N. Jiang, W. Pan, B. Luo, W. L. Zhang, and D. Zheng, Chin. Opt. Lett. **6**, 517 (2008).
[5] X. F. Li, W. Pan, B. Luo, and D. Ma, IEEE J. Quantum Electron. **42**, 953 (2006).
[6] W. L. Zhang, W. Pan, B. Luo, X. H. Zou, M. Y. Wang, and Z. Zhou, Opt. Lett. **33**, 237 (2008).
[7] R. Mislovaty, E. Klein, I. Kanter, and W. Kinzel, Phys. Rev. Lett. **91**, 118701 (2003).
[8] X. F. Li, W. Pan, B. Luo, and D. Ma, J. Lightwave Technol. **24**, 4936 (2006).
[9] A. Argyris, D. Syvridis, L. Larger, V. Annovzzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature (London) **437**, 343 (2005).
[10] J. Mulet, C. Masoller, and C. R. Mirasso, Phys. Rev. A **65**, 063815 (2002).
[11] R. Vicente, I. Fischer, and C. R. Mirasso, Phys. Rev. E **78**, 066202 (2008).
[12] F. Rogister and M. Blondel, Opt. Commun. **239**, 173 (2004).
[13] T. Heil, I. Fischer, W. Elsasser, J. Mulet, and C. R. Mirasso, Phys. Rev. Lett. **86**, 795 (2001).
[14] E. Klein, N. Gross, M. Rosenbluh, W. Kinzel, L. Khaykovich, and I. Kanter, Phys. Rev. E **73**, 066214 (2006).
[15] E. Klein, N. Gross, E. Kopelowitz, M. Rosenbluh, L. Khaykovich, W. Kinzel, and I. Kanter, Phys. Rev. E **74**, 046201 (2006).
[16] R. Vicente, C. R. Mirasso, and I. Fischer, Opt. Lett. **32**, 403 (2007).
[17] N. Jiang, W. Pan, L. S. Yan, B. Luo, L. Yang, S. Y. Xiang, and D. Zheng, Opt. Commun. **282**, 2217 (2009).
[18] M. C. Chiang, H. F. Chen, and J. M. Liu, Opt. Commun. **261**, 86 (2006).
[19] E. Klein, R. Mislovaty, I. Kanter, and W. Kinzel, Phys. Rev. E **72**, 016214 (2005).
[20] I. Kanter, N. Gross, E. Klein, E. Kopelowitz, P. Yoskovits, L. Khaykovich, W. Kinzel, and M. Rosenbluh, Phys. Rev. Lett. **98**, 154101 (2007).
[21] D. Kanakidis, A. Argyris, A. Bogris, and D. Syvridis, J. Lightwave Technol. **24**, 335 (2006).
[22] M. C. Soriano, F. Ruiz-Oliveras, P. Colet, and C. R. Mirasso, Phys. Rev. E **78**, 046218 (2008).
[23] A. S. Landsman and I. B. Schwartz, Phys. Rev. E **75**, 026201 (2007).
[24] M. C. Chiang, H. F. Chen, and J. M. Liu, IEEE J. Quantum Electron. **41**, 1333 (2005).
[25] J. Ohtsubo, IEEE J. Quantum Electron. **38**, 1141 (2002).
[26] A. Bogris, P. Rizomiliotis, K. E. Chlouverakis, A. Argyris, and D. Syvridis, IEEE J. Quantum Electron. **44**, 119 (2008).
[27] A. Murakami and K. A. Shore, Phys. Rev. A **72**, 053810 (2005).
[28] J. Paul, M. W. Lee, and K. A. Shore, Opt. Lett. **29**, 2497 (2004).
[29] A. B. Wang, W. C. Wang, and H. C. He, IEEE Photonics Technol. Lett. **20**, 1633 (2008).
[30] A. Bogris, D. Kanakidis, A. Argyris, and D. Syvridis, IEEE J. Quantum Electron. **40**, 1326 (2004).
[31] D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, Opt. Lett. **32**, 2960 (2007).
[32] D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, IEEE J. Quantum Electron. **45**, 879 (2009).
[33] M. W. Lee, P. Rees, K. A. Shore, S. Ortin, L. Pesquera, and A. Valle, IEE Proc.: Optoelectron. **152**, 97 (2005).